Guidance for Completion of the Security and Privacy Section Of Exhibit 300, *Capital Asset Plan and Business Case*

What is the purpose of this guidance?

This guidance provides suggestions for the acceptable completion of Part II, Section II.B, of the Exhibit 300, the Capital Asset Plan and Business Case." Completion of Exhibit 300 is described in OMB Circular A-11, Part 7, *Planning, Budgeting, Acquisition, and Management of Capital Assets*.

What information does DOC recommend be addressed in Section II.B of the Exhibit 300?

In your responses to the first four questions on Security and Privacy (item II.B.5 is self-explanatory), describe for OMB the system security controls in familiar terms – DOC recommends the terms used in NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems* (http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf). This guidance describes security in terms of three control areas (Management, Operational, and Technical) that comprise the 17 critical element areas (see NIST Special Publication 800-26, section 3.2, pages 9-11). You may use the three control areas and/or the 17 critical elements to describe more specifically your planned and implemented efforts. Specifically,

- Question II.B.1: Explain how security is provided and funded for the investment project. Include a description of the key security controls. These controls should be described briefly, either by the overall control areas (Management Controls, Operational Controls, and Technical Controls) or by selecting key critical elements from the list of 17 critical elements in. Select elements that are not discussed in section II.B.2. For example, under Management Controls, describe the process for periodic review of security controls (critical element 2) and how security is considered in the project's life cycle (element 3). Under Operational Controls, describe the process for physical and environmental protection (element 7), production controls (element 8), and contingency planning (element 9). For Technical Controls, describe how identification and authentication provides security (element 15).

- Question II.B.1.A: State the dollar amount specifically allocated for this investment's IT security, and indicate whether or not the amount is an increase of IT security funding to remediate vulnerabilities found through audit or self-assessment. FISMA requires that Project Managers integrate funding for the investment's IT security controls into the life cycle cost of all IT investments. This funding must be adequate to mitigate weaknesses in IT security identified through annual self-assessments performed in accordance with NIST Special Publication 800-26 and through periodic security evaluations by external entities.

- Question II.B.2 and sub-questions A through F: Provide clear, descriptive, and concise responses to each question. In the FY 05 process, OMB put on the watch list every investment that failed to provide a recent date or adequate explanation to these questions.

  – II.B.2.A: An up-to-date security plan is one that was revised after the last major system update or within three years of the current date, whichever is more recent. If a plan exists, provide its date and whether the plan complies with requirements of OMB and NIST guidance namely OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources* http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html), and NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, (http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF). If an up-to-date, compliant plan does not exist, explain why and provide the target completion date for the plan.

- II.B.2.B: State whether the investment project has undergone certification and accreditation and specify the methodology used. For the methodology, DOC requires use of the National Information Assurance Certification and Accreditation Process (NIACAP), and recommends supplemental implementation guidance issued by NIST in Special Publication 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems* (http://csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf). Specify the title of the program official serving as the designated approving authority (DAA). State whether or not a certification was completed, and if the system has received full or interim accreditation to operate. OMB requires that systems have a full, not interim, authority to operate in order to fully satisfy this requirement. If the system has a full accreditation (authority to operate), state the date the accreditation was granted. If full certification and/or accreditation is not complete (for example, for new systems under development), explain why and provide the target completion date for full certification and accreditation.

- II.B.2.C: State whether the investment project's management, operational, and technical controls have been tested for effectiveness. Describe whether OIG, GAO, or the DOC Compliance Review Program has audited the investment project. Such audits examine and test the effectiveness and adequacy of management, operational, and technical controls in accordance with GAO's Federal Information System Controls Audit Manual. Also, describe all internal self-assessments performed (e.g., quarterly vulnerability scans, completion of the NIST 800-26 self-assessment checklist annually, etc.).

- II.B.2.D: State whether system users have completed training in general IT security concepts as well as system specific security training. Describe the nature of the IT security training provided (e.g., Web-based training, read-and-sign agreements, warning banners on system logon) and its frequency. DOC requires general IT security training at entry-on-duty, and annual refresher training thereafter. System-specific training and update of user agreements are the determination of the system owner. Describe any user manuals developed and distributed to system users, and specify whether training includes briefing users on the system rules of behavior and consequences of non-compliance.

- II.B.2.E: Describe how incident handling capabilities have been designed into the project. DOC recommends a three-pronged response that addresses prevention, detection, and correction/resumption.

  - First, describe the implementation of specific operational and technical controls that detect intrusions into the project's computing environment, and how such detections are handled. Begin with a statement that security is a priority, therefore controls have been strengthened, implemented, or are planned to prevent the opportunity for intrusion (cite one or two examples).

- Next, describe the detection capabilities in terms of established policies and procedures (provide dates issued and topics covered), use of audit logs (describe key events captured and frequency of review), technical devices (type of intrusion detection sensors installed and frequency of monitoring). Add that incidents are reported to the DOC Computer Incident Response Team (CIRT), or an operating unit-specific CIRT, as appropriate, which in turn reports incidents to the Federal Computer Incident Response Center (FedCIRC)/US-CERT.

- Conclude by describing the procedures in place to recover from minor and major interruptions in service or loss of data after an incident has been detected, isolated, and terminated, as well as the frequency of testing the recovery plan.

– II.B.2.F: Specify whether contractors operate the system, and, if so, from on-site or off-site. If contract services are included in system support, DOC requires application of Commerce Acquisition Manual (CAM) section 1337.70, *Security Processing Requirements for On-Site Service Contracts*, and related CAM Notice 00-02 (http://oamweb.osec.doc.gov/app/cam.htm). These provide facility access criteria and contract language for IT service contracts. In addition, DOC recommends use of National Institute of Standards and Technology (NIST) Special Publication 800-4, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*, which provides additional guidance for security considerations in procurements.

- Question II.B.3: State whether the investment project permits public access. If the project permits public access, describe the operational and technical controls in place to protect privacy (also see the earlier Q&A on “Privacy Impact Assessment”).

- Question II.B.4: State whether the investment project collects, uses, processes, transmits, or stores personal information. If so, state the reason and describe the policies and procedures in place to ensure the proper handling of personal information.

What if I need more help in preparing Section II.B of the Exhibit 300?

DOC recommends that you consult with the system and IT security professionals knowledgeable with the specific project/system described in the Exhibit 300. In addition, your IT Security Officer and the DOC OCIO’s IT Security Program Team can also assist you to respond to the questions in Section II.B of Exhibit 300.